UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,960	08/02/2001	Bruno Couillard	47-15 US	4262

25319 7590 12/28/2005

FREEDMAN & ASSOCIATES
117 CENTREPOINTE DRIVE
SUITE 350
NEPEAN, ONTARIO, K2G 5X3
CANADA

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 12/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/919,960	COUILLARD, BRUNO	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 September 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.

2. Amendment filed on 11/14/2005 has been received and considered.

Drawings

3. The drawings filed 09/24/2002 have been reviewed and accepted.

Claim Rejections - 35 USC § 112

4. The rejections under the second paragraph of 35 U.S.C. 112 have been withdrawn based on the filed amendments.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-9 and 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier (Applied Cryptography), in view of Ober et al (US 6307936), further in view of Arnold (US 6175924) and further in view of Fischer (US 6141423).

As per claims 1-3 and 15, Schneier discloses a method for transferring a key by encrypting the first electronic key using a first encryption key of the key provider; transferring the encrypted first electronic key from the key provider system to the second other system via the information network; and decrypting the encrypted first electronic key using the second encryption key stored within the first secure module and to store the decrypted first electronic key wherein the second encryption key is only for decrypting encrypted electronic keys (see section 8.3) and the key encrypting keys should be of greater length than the key it is encrypting (see page 177 and pages 166-167).

Schneier fails to disclose the three different keys; the encrypting and decrypting being performed in a secure module containing a processor and ROM; and the keys being un-modifiable and un-accessible outside of the module.

However, Ober et al teaches three different levels of keys (see column 3 lines 1-22 where the LSV is the super root key, the GKEK is the root key and the remaining keys are the private keys) Arnold teaches a secure module components (see column 3 lines 48-61) and Fischer teaches the properties of the keys (see column 4 line 56 through column 5 line 7).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use three levels of keys and Arnold's secure module with the properties of Fischer in the key transferring system of Schneier.

Motivation to do so would have been to provide a comprehensive powerful and secure encryption key management scheme (see Ober et al column 1 lines 49-51) to efficiently execute encryption algorithms (see Arnold column 3 lines 48-61) and to protect against contamination (see Fischer column 4 line 56 through column 5 line 7).

As per claims 4 and 16-18, the modified Schneier, Ober et al, Arnold and Fischer system discloses the processor internal to the module accesses the second encryption key only in response to a request from a corresponding secure module (as rejected above where it is implied that since the key is only used to encrypt other keys it wouldn't be used unless it is requested and as rejected in claims above).

As per claims 5-6, the modified Schneier, Ober et al, Arnold and Fischer system discloses using asymmetric and symmetric keys (see Arnold column 3 lines 48-61).

As per claims 7-8, the modified Schneier, Ober et al, Arnold and Fischer system discloses generating a first electronic key within a key-generating processor internal to the

key provider system within a secure module (see Schneier section 8.3 in the secure module of Arnold).

As per claim 9, the modified Schneier, Ober et al, Arnold and Fischer system discloses the first electronic key is a root key for use in at least one of encrypting and decrypting private encryption keys (see Schneier section 8.3).

7. Claims 10-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold and Fischer system as applied to claims 1, 6 and 15 above, and further in view of Spelman et al (US 5680458).

As per claims 10, the modified Schneier, Ober et al, Arnold and Fischer system fails to disclose second and third encryption keys being stored.

However, Spelman et al teaches such keys (see column 2 lines 4-17 where the second and third keys are of the plurality of keys).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store Spelman et al's keys in the modified Schneier, Ober et al, Arnold and Fischer system.

Motivation to do so would have been to have more than one root key (see Spelman et al column 2 lines 4-17).

As per claim 11, the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system discloses encrypting a fourth encryption key using one of the third encryption key and a key corresponding to the third encryption key; transferring the encrypted fourth encryption key from the key provider system to the second other system via the information network; providing the encrypted fourth encryption key to the processor internal to the first secure module of the second other system; and, executing program code on the processor internal to the first secure module to decrypt the encrypted fourth encryption key using the third encryption key stored within the memory circuit of the first secure module and to store the decrypted fourth encryption key within the memory circuit of the first secure module at a location corresponding approximately to the location where the second encryption key was stored (see Schneier and Arnold as applied to Spelman et al's key).

As per claim 12-13, the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system discloses replacing the second and third keys (see Spelman et al column 2 lines 4-17) and root key encrypting keys (see Spelman et al's keys as applied to Schneier and Arnold's key exchange system).

As per claim 14, the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system discloses erasing the second

encryption key from a first storage area of the memory circuit; and, storing the decrypted fourth encryption key within approximately the same first storage area of the same memory circuit (see Spelman et al column 2 lines 4-17 where it is implied that a replaced key is erased).

8. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold and Fischer system as applied to claim 18 above, and further in view of Easter et al (US 559889).

As per claim 19 the modified Schneier, Ober et al, Arnold and Fischer system fails to disclose the module is FIPS 140 compliant.

However, Easter et al teaches such a compliant module (see column 6 lines 13-21).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to have the module of the modified Schneier, Ober et al, Arnold and Fischer system be FIPS 140 compliant.

Motivation to do so would have been to allow for top security (see Easter et al column 6 lines 13-21).

9. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold,

Fischer and Easter et al system as applied to claim 19 above, and further in view of Bergum et al (US 5249277).

As per claim 20, the modified Schneier, Ober et al, Arnold, Fischer and Easter et al system fails to disclose a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

However, Bergum et al teaches such a method of tamper protection (see column 4 lines 7-32).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to apply this method of tamper protection to the modified Schneier, Ober et al, Arnold, Fischer and Easter et al system.

Motivation to do so would have been to provide maximum key security (see Bergum et al column 4 lines 7-32).

10. Claims 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system as applied to claim 10 above, and further in view of Mason et al (US 6331784).

As per claims 21-24 the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system discloses the claimed

limitations as in claim 10 above, but fails to disclose the keys only being erasable by the program code.

However, Mason et al teaches a system with an erase only mode (see column 2 lines 39-47).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate Mason et al's erase only mode in the modified Schneier, Ober et al, Arnold, Fischer and Spelman et al system.

Motivation to do so would have been so no information can be read from the device (see Mason et al column 2 lines 39-47).

11. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, and Mason et al system as applied to claim 24 above, and further in view of Ehrsam et al (US 4386234).

As per claim 25, the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, and Mason et al system fails to disclose the substantially non-volatile reprogrammable memory circuit is one of an electrically erasable read-only memory circuit and a random access memory circuit having an on-board power supply in the form of a battery. However, Ehrsam et al teaches such a memory having a battery (see column 13 lines 45-50).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Ehrsam et al's battery powered memory in the modified Schneier, Arnold, Fischer, Spelman et al, and Mason et al key exchange system.

Motivation to do so would have been to enable key retention when terminal power may not be present (see Ehrsam et al column 13 lines 45-50).

12. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, Mason et al, and Ehrsam et al system as applied to claim 25 above, and further in view of Easter et al (US 559889).

As per claim 26 the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, Mason et al, and Ehrsam et al system fails to disclose the module is FIPS 140 compliant.

However, Easter et al teaches such a compliant module (see column 6 lines 13-21). At the time of the invention it would have been obvious to a person of ordinary skill in the art to have the module of the modified Schneier, Arnold, Fischer, Spelman et al, Mason et al, and Ehrsam et al system be FIPS 140 compliant. Motivation to do so would have been to allow for top security (see Easter et al column 6 lines 13-21).

13. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, Mason et al, Ehrsam et al, and Easter system as applied to claim 26 above, and further in view of Bergum et al (US 5249277).

As per claim 27, the modified Schneier, Ober et al, Arnold, Fischer, Spelman et al, Mason et al, Ehrsam et al, and Easter system fails to disclose a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion. However, Bergum et al teaches such a method of tamper protection (see column 4 lines 7-32).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to apply this method of tamper protection to the modified Schneier, Arnold, Spelman et al, Ehrsam et al, and Easter et al system.

Motivation to do so would have been to provide maximum key security (see Bergum et al column 4 lines 7-32).

Response to Arguments

14. Applicant's arguments with respect to claims 1-27 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Richards (US 6069957) and Wasilewski et al (US 6424714) teach that key encrypting keys should be longer than the keys they encrypt.

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137